Opening Statement of the Honorable Mary Bono Mack
Subcommittee on Commerce, Manufacturing, and Trade
"Understanding Consumer Attitudes About Privacy"
October 13, 2011
(As Prepared for Delivery)

When it comes to online privacy – at least for me – consumer attitudes and expectations are the bits and bytes that matter the most.

Do Americans really believe enough is being done today to protect their online privacy? Are they taking advantage of the many privacy tools currently available to them? Do they even know about these tools? If not, then why not? And do these privacy features – for the most part – really work? Or is it time for Congress to finally legislate in this area?

This is a hearing that I have been looking forward to for a long time, because it's the first time we have tried to quantify what consumers expect and want. This is where the "rubber hits the road" with respect to online privacy.

Today, there is no single federal law expressly governing all data collection in the United States. Instead, there is a confusing hodge-podge of more than 300 state and federal laws. Likewise, there is no single regulator to enforce all of these privacy-related laws. Rather, an industry-specific approach has emerged whereby Congress has restricted consumer data collection and use by subject matter and provided the enforcement authority to the relevant federal agency.

As it stands today, the Federal Trade Commission arguably has the broadest jurisdiction to enforce general privacy violations under its section 5 authority defining unfair or deceptive acts or practices. Since 2001, the Commission has brought 34 cases against companies that failed to protect consumer information, including when companies fail to adhere to their own stated privacy policy.

In recent years, both policymakers and stakeholders have expressed increasing concerns regarding the collection and availability of consumers' personal information online. Increased data collection and storage by websites, information brokers, direct marketers, ISPs, and advertisers have been driven in large part by the rapid decline of the associated costs of data processing and storage, while at the same time the value of consumer information has increased significantly.

As we know, data about consumers' online behavior is being used today to target ads, increasing the likelihood of a sale of a particular product. Is this bad? Not necessarily. But is this process transparent enough and do consumers have enough information and tools available to them to be able to opt out of having their data collected and shared with unknown parties if they so choose?

In many ways, this is the root of the privacy issue.

In response to growing concerns over online data collection and use – particularly regarding behavioral advertising – the online advertising community developed a self-regulatory model to provide consumers with notice and choice about advertisements delivered to them through behavioral targeting.

The Digital Advertising Alliance developed and implemented the so-called "About Ads" to provide consumers more information on why they are seeing a particular ad and to provide them a mechanism to opt out of future ads directed at them based on behavioral advertising.

Later, the FTC took things a step further, proposing a number of principles to enhance consumer choices regarding privacy, including the concept of a "Do-Not-Track" mechanism.
Since a hearing in the last Congress on "Do-Not-Track" legislation, the two most popular browser developers – Microsoft's Internet Explorer and Mozilla's Firefox - have both designed and incorporated a "Do-Not-Track" feature into their browsers.

These features are user-controlled so consumers must choose to turn them on to actually prevent tracking. Internet Explorer blocks content from sites that are on tracking protection lists and that could otherwise use the content to collect information, while Mozilla's Firefox broadcasts a signal to each website a consumer actually visits, communicating the consumer's desire not to have his or her information collected.

Clearly, the effectiveness of Mozilla's approach faces significant hurdles because every website that receives the signal from the consumer's browser must choose to honor the request, and currently there is no requirement that websites must do so.

So what do consumers think about all of this? And when it comes to the Internet, how do we – as Congress and as Americans – balance the need to remain innovative with the need to protect privacy?

Clearly, the explosive growth of technology has made it possible to collect information about consumers in increasingly sophisticated ways. Sometimes the collection and use of this information is extremely beneficial; other times, it's not.

Despite everything that I have heard in our previous hearings, I still remain somewhat skeptical right now of both industry and government. Frankly, I don't believe industry has proven that it's doing enough to protect American consumers, while government, unfortunately, tends to overreach whenever it comes to new regulations.

That's why I'm so anxious today to hit the "refresh key" to learn the latest about consumer attitudes and expectations.

###